

SSS:JV
F.#2019R01253

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
A BLACK APPLE IPHONE, IMEI NO.
359405083064715, AND A BLACK LG
WIRELESS PHONE, IMEI NO.
354064082370394, CURRENTLY WITHIN
THE CUSTODY OF THE UNITED
STATES POSTAL INSPECTION
SERVICE IN THE EASTERN DISTRICT
OF NEW YORK

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. 19-M-1140

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, LOUIS A. MAIOCCO, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (“USPIS”). I am presently assigned to the Brooklyn Mail Theft Team. I have been involved in the investigation of numerous cases involving mail theft. As part of those investigations, I have made arrests, interrogated subjects, collected evidence and interviewed witnesses. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the owner of the phone’s

criminal history record; and reports from, and conversations with, other law enforcement officers involved in the investigation.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a black Apple iPhone, IMEI No. 359405083064715, and a black LG wireless phone, IMEI No. 354064082370394, belonging to Patrick Hernandez (the “Devices”). The Devices are currently in the possession of the USPS within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Hendry Grullon, Justin Delacruz and Patrick Hernandez (the “Defendants”) committed violations of federal criminal law, to wit, did knowingly and intentionally conspire to commit postal theft in violation of 18 U.S.C. § 371, and did knowingly and intentionally commit postal theft in violation of 18 U.S.C. § 1708. There is also probable cause to search the Devices described in Attachment A for evidence, instrumentalities, contraband and/or fruits of this crime, further described in Attachment B.

7. Based on my training and experience, I have learned some of the methods by which individuals steal mail from United States Postal Service (“USPS”) collection boxes. I

have learned, among other things, that small, hand-held objects like CDs, bottles, rat traps, and other items which are covered in sticky residue, are often used to extract mail (i.e., “fish”) from USPS collection boxes. Mail thieves then remove checks, money orders and other items of value from the extracted mail.

The 65th Street and 12th Avenue Postal Theft and Arrest

8. On or about September 12, 2019, at approximately 5:25 a.m., a New York City Police Department (“NYPD”) officer (hereinafter, “Officer-1”)¹ on patrol observed a black sedan vehicle (the “Vehicle”) pull up next to a USPS collection box (“Mailbox-1”) located at the corner of 65th Street and 12th Avenue in Brooklyn, New York. After observing two male individuals leave the Vehicle, an individual later identified as Hendry Grullon was observed approaching Mailbox-1 and placing something inside of Mailbox-1. Grullon then walked away from Mailbox-1 and returned to it and appeared to retrieve an item resembling a bottle. By his behavior, the second male individual, later identified as Justin Delacruz, appeared to be acting as a lookout. Officer-1 observed Grullon and Delacruz return to the Vehicle.

9. Officer-1 notified other NYPD officers in the area of his/her observations, and other officers responded to the area of 65th Street and 12th Avenue. Multiple NYPD officers approached the Vehicle, including Officer-1. Officer-1 and another officer (“Officer-2”)

¹ Because multiple law enforcement personnel were involved in the arrest of this defendants, I refer to them as Officer-1 and Officer-2. The identities of each of these individuals are known to the affiant, and I have interviewed Officer-1, Officer-2 and other law enforcement officers about the events set forth herein.

observed a bottle with a shoe string tied on to it on the floor of the Vehicle. In addition, Officer-1 and Officer-2 observed a third male individual in the Vehicle, later identified as Patrick Hernandez, the owner of the Devices.

10. The NYPD officers instructed Delacruz, Grullon and Hernandez to leave the Vehicle and all three were placed under arrest.

11. The defendants were transported to the NYPD's 68th Precinct for processing. During a search of Delacruz at the station house, officers recovered checks and money orders hidden inside of Delacruz's shoe. The two Devices were also seized from Hernandez incident to his arrest.

12. During an inventory search of the Vehicle at the station house, Officer-1 found checks and money orders stashed in the driver's side door of the Vehicle. Additional checks were found under the mat of a rear seat of the Vehicle. The recovered checks and money orders did not belong to and were not made out to the defendants. The Vehicle is owned by Hernandez, the owner of the Devices.

13. After being advised of his Miranda rights, Hernandez consented to be interviewed and admitted that he knew that Grullon and Delacruz were "fishing" – the colloquial term for theft from mailboxes.

The Clarendon Road and Nostrand Avenue Postal Theft

14. After I learned of the foregoing incident, USPIS Analysts contacted some of the victims whose names appeared on the checks or money orders to determine where those victims had mailed the items. Based on these interviews, USPIS Analysts identified locations in Flatbush, Brooklyn, where multiple checks had been mailed. Inspectors

obtained video of surveillance capturing two postal boxes located in the Flatbush area (“Mailbox-2” and “Mailbox-3”) in the early morning hours of September 12, 2019.

Inspectors, among other things, observed on video surveillance a black sedan consistent in appearance with the Vehicle, pull up near both Mailbox-2 and Mailbox-3. Multiple male individuals can be seen leaving the black sedan vehicle, and one appeared to place an item into both Mailbox-2 and Mailbox-3 to attempt to fish items out of the mailboxes. On the videos, I was able to observe individuals who resemble Grullon and Hernandez. There also appears to be a third individual in some of the videos. Based on my observations of the individuals and vehicle, the overlap in time between the mailbox fishing in Flatbush and the incident at 65th Street and 12th Avenue, and my investigation to date, I believe it was the defendants who attempted to steal mail from both Mailbox-2 and Mailbox-3, as captured on video surveillance footage.

15. Mailbox-2 is located near the corner of Clarendon Road and Nostrand Avenue, in Brooklyn, New York. The area is well-lit and under surveillance by multiple cameras. The video surveillance of Mailbox-2 shows Hernandez speaking on a wireless phone in the immediate vicinity of Mailbox-2. Based on my training and experience, Hernandez appears to be scouting the area around Mailbox-2 and acting as a lookout. From approximately 1:30 a.m. to 2:15 a.m. on September 12, 2019, Hernandez is in the general vicinity of Mailbox-2 while Grullon repeatedly approaches and interacts with Mailbox-2, including “fishing” mail from Mailbox-2 on multiple occasions. Video surveillance also shows Hernandez joining Grullon after he takes the stolen mail from the mailbox.

The TD Bank Deposits

16. As part of the investigation, USPIS Analysts and Investigators learned of deposits of stolen money orders that had been endorsed and deposited into a TD Bank account registered to a Patrick Hernandez, the owner of the Devices.

17. Video surveillance recordings provided by TD Bank show Patrick Hernandez depositing stolen money orders on June 30, July 13, August 5 and August 22. The purchasers of the money orders told the USPS Investigators that they had mailed the money orders, depositing the letters containing the money orders into USPS collection boxes in Brooklyn, and that Hernandez was not the intended recipient of that mail or those money orders.

Arrests and Indictment

18. On Saturday, September 13, 2019, the defendants were arrested pursuant to a federal complaint (Dkt. No. 19-MJ-821).

19. On October 11, 2019, a grand jury within the Eastern District of New York returned an indictment against Justin Delacruz (Dkt. No. 19-CR-464 (ILG)).

20. Based on my training and experience, individuals who coordinate illegal activity typically use phones to plan and coordinate the crime. In particular, in this case, based on my training, experience, review of surveillance and interviews with witnesses, it is my belief that Hernandez called and/or messaged Grullon and Delacruz to plan and/or coordinate postal theft.

21. Also based on my training and experience, historical financial information, such as bank records, checks, credit card bills, account information, and other financial

records may evidence a motive to commit a crime and/or the disposition of stolen mail, and articles abstracted from therein, including checks and money orders.

22. Also based on my training and experience, wireless phones contain GPS and location data that can be used to establish a defendant's presence at the scene of the crime.

23. The Devices are currently in the lawful possession of the USPIS. The Devices that were in the possession of Hernandez were seized incident to his state arrest on September 12, 2019. While the USPIS may already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

24. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the USPIS.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of

calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store

other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and using computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that may serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence may be on the Devices because:

- h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- i. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- k. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- l. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that may expose

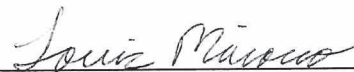
many parts of the Devices to human inspection to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Louis A. Maiocco
United States Postal Inspection Service

Subscribed and sworn to before me
on ~~December 5, 2019~~: December 6, 2019



HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is a black Apple iPhone, IMEI No. 359405083064715, and a black LG wireless phone, IMEI No. 354064082370394, belonging to Patrick Hernandez (the “Devices”). The Devices are currently in the possession of the USPIS within the Eastern District of New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 371 and 1708 (the “SUBJECT OFFENSES”) involving Justin Delacruz, Hendry Grullon and Patrick Hernandez since on or about June 30, 2019, including:

- a. Lists of, and/or contact information for, individuals with who Patrick Hernandez discussed the Subject Offenses, including planning and coordinating the, and related identifying information;
- b. Any communications regarding the SUBJECT OFFENSES, or the planning thereof;
- c. any information related to the SUBJECT OFFENSES (including names, addresses, phone numbers, or any other identifying information of individuals);
- d. photographs, video, text messages, instant messages and all other electronic communications, saved audio files, web browsing history and other records regarding the SUBJECT OFFENSES;
- e. records of or information about the Devices’ Internet activity regarding the SUBJECT OFFENSES, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- f. statements and other information regarding the SUBJECT OFFENSES;
- g. communications with Hendry Grullon and Patrick Hernandez;

- h. evidence of the times the Devices were used, to include information recording Patrick Hernandez's schedule or travel from June 1, 2019 through September 12, 2019;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the Devices;
 - j. geolocation data from June 1, 2019 through September 12, 2019; and
 - k. all bank records, checks, credit card bills, account information, and other financial records from June 1, 2019 through September 12, 2019.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.